Amendment to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

1. (currently amended) An apparatus for accessing material, comprising:

a secure registry encrypted with a registry key that was generated by using an identification of an authorized entity, and storing another key useful for decrypting material; and

a control module configured to regenerate said registry key by using an identification of a current entity associated with said secure registry at the time of said regeneration, and decrypt said secure registry using said regenerated registry key for retrieval of said another key ~~if a correct entity identification is received~~ provided the identifications of said authorized and current entities are the same.

2. (original) The apparatus according to claim 1, wherein said control module receives said material as streaming media, and is further configured to decrypt said material using said another key.

3. (original) The apparatus according to claim 2, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and said control module receives said at least one content key encrypted with said another key.

4. (original) The apparatus according to claim 3, wherein said another key comprises at least one license key corresponding to a license to use said material.

5. (original) The apparatus according to claim 2, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and said control module receives said at least one content key encrypted with a public key of said apparatus.

6. (original) The apparatus according to claim 5, wherein said another key comprises a private key of said apparatus.

7. (original) The apparatus according to claim 1, further comprising a file including an encrypted version of said material, and said another key is useful for decrypting said encrypted version of said material.

8. (original) The apparatus according to claim 7, wherein said material is in MPEG-4 format encrypted with at least one content key, and said at least one content key is provided encrypted with said another key.

9. (original) The apparatus according to claim 8, wherein said another key comprises at least one license key corresponding to a license to use said material.

10. (original) The apparatus according to claim 7, wherein said material is in MPEG-4 format encrypted with

at least one content key, and said at least one content key is provided encrypted with a public key of said apparatus.

11. (original) The apparatus according to claim 10, wherein said another key comprises a private key of said apparatus.

12. Cancelled.

13. Cancelled.

14. Cancelled.

15. Cancelled.

16. Cancelled.

17. Cancelled.

18. Cancelled.

19. (currently amended) The apparatus according to claim [[18]] 1, wherein said ~~sensed entity~~ identification of said current entity is unique for said apparatus.

20. Cancelled.

21. Cancelled.

22. Cancelled.

23. Cancelled.

24. (currently amended) The apparatus according to claim [[23]] 19, wherein said ~~sensed entity~~ identification of said current entity is a computer identification.

25. (currently amended) The apparatus according to claim [[23]] 19, wherein said ~~sensed entity~~ identification of said current entity is a network interface card identification.

26. (currently amended) The apparatus according to claim [[23]] 19, wherein said ~~sensed entity~~ identification of said current entity is a hard disk drive identification.

27. (currently amended) The apparatus according to claim [[22]] 1, wherein said ~~sensed entity~~ identification of said current entity is unique for a hardware device connectable to said apparatus.

28. (currently amended) The apparatus according to claim 27, wherein said ~~sensed entity~~ identification of said current entity is a smartcard identification.

29. (currently amended) The apparatus according to claim 27, wherein said ~~sensed entity~~ identification of said current entity is a content storage unit identification.

30. (currently amended) The apparatus according to claim [[22]] 1, wherein said ~~sensed entity~~ identification of said current entity is unique to a user of said apparatus.

31. (currently amended) The apparatus according to claim 30, wherein said ~~sensed entity~~ identification of said current entity is a credit card number.

32. (currently amended) The apparatus according to claim 30, wherein said ~~sensed entity~~ identification of said current entity is a predefined user identification.

33. (currently amended) The apparatus according to claim 30, wherein said ~~sensed entity~~ identification of said current entity is a biometrics based identification.

34. (original) The apparatus according to claim 33, wherein said biometrics based identification is a fingerprint of said user of said apparatus.

35. (original) The apparatus according to claim 33, wherein said biometrics based identification is a speech of said user of said apparatus.

36. Cancelled.

37. (original) The apparatus according to claim 1, wherein said control module comprises a processor and a control program running on said processor.

38. (original) The apparatus according to claim 1, wherein said control module includes logic circuitry.

39. (original) The apparatus according to claim 1, wherein said control module is license-enabled to a unique identification of said apparatus.

40. (original) The apparatus according to claim 1, wherein said secure registry further stores information related to said material.

41. (original) The apparatus according to claim 40, wherein said information related to said material includes usage rights included in a license for said material.

42. (currently amended) A method for accessing material, comprising:

receiving a secure registry that has been encrypted with a registry key that was generated by using an identification of an authorized entity;

regenerating said registry key using an identification of an entity associated with said secure registry at the time of said regeneration;

decrypting [[a]] said secure registry with [[a]] said regenerated registry key;

retrieving another key from said decrypted secure registry; and

decrypting encrypted material using said another key to access said material.

43. (original) The method according to claim 42, further comprising receiving said encrypted material as streaming media.

44. (original) The method according to claim 43, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with said another key.

45. (original) The method according to claim 44, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key; and

decrypting said encrypted material with said at least one content key to access said material.

46. (original) The method according to claim 45, wherein said another key comprises at least one license key corresponding to a license to use said material.

47. (original) The method according to claim 43, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with a public key of a recipient of said material.

48. (original) The method according to claim 47, wherein said another key comprises a private key of said recipient of said material.

49. (original) The method according to claim 48, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said private key; and

decrypting said encrypted material with said at least one content key to access said material.

50. (original) The method according to claim 42, further comprising receiving said encrypted material as a file.

51. (original) The method according to claim 50, wherein said file is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with said another key.

52. (original) The method according to claim 51, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key; and

decrypting said encrypted material with said at least one content key to access said material.

53. (original) The method according to claim 52, wherein said another key comprises at least one license key corresponding to a license to use said material.

54. (original) The method according to claim 50, wherein said file is in MPEG-4 format encrypted with at

least one content key, and further comprising receiving said at least one content key encrypted with a public key of a recipient of said material.

55. (original) The method according to claim 54, wherein said another key comprises a private key of said recipient of said material.

56. (original) The method according to claim 55, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said private key; and

decrypting said encrypted material with said at least one content key to access said material.

57. Cancelled.

58. Cancelled.

59. Cancelled.

60. Cancelled.

61. Cancelled.

62. Cancelled.

63. Cancelled.

64. Cancelled.

65. Cancelled.

66. (currently amended) The method according to claim [[65]] 42, wherein said ~~sensed entity~~ identification of said entity is unique to a host.

67. (currently amended) The method according to claim [[65]] 42, wherein said ~~sensed entity~~ identification of said entity is unique to a hardware device connectable to a host.

68. (currently amended) The method according to claim [[65]] 42, wherein said ~~sensed entity~~ identification of said entity is unique to a user of a host.

69. (currently amended) The method according to claim 68, further comprising receiving said ~~sensed entity~~ identification of said entity from information entered into an input device by said user.

70. (original) The method according to claim 69, wherein said input device is a keyboard.

71. (original) The method according to claim 69, wherein said input device is a biometrics device.

72. (original) The method according to claim 42, further comprising after said decrypting encrypted material using said another key to access said material:

using said material according to a license stored in said secure registry along with said another key.